IDA

**Joint
Advanced
Warfighting
Program**

INSTITUTE FOR DEFENSE ANALYSES

Lessons Learned: Commanding a Digital Brigade Combat Team

Colonel (P) Rick Lynch, USA

20011017 017

INSTITUTE FOR DEFENSE ANALYSES
Joint Advanced Warfighting Program

Lessons Learned: Commanding a Digital Brigade Combat Team

Colonel (P) Rick Lynch, USA

June 30, 2001

Colonel (P) Rick Lynch, USA, came to the Joint Advanced Warfighting Program from command of 1ˢᵗ Brigade Combat Team, 4ᵗʰ Infantry Division, the Army's digital and experimental brigade during that period. This paper is a personal statement of the insights and lessons that he drew from that experience.

While the paper is not the usual JAWP product directly addressing a joint issue, it is relevant beyond the boundaries of a Brigade Combat Team and deserves a wider audience. One reason is that the operational content Rick wrestled with as Brigade Commander is largely about harnessing the great potential of situation understanding shared among elements of a force. This is a notion fundamental to network-centric thinking and emerging concepts in other Services and in the joint community. Furthermore, the relevance of his experiences with the processes of experimentation, spiral development, and the co-evolution of doctrinal, organizational, training and people dimensions, along with the materiel, also extends beyond the Army. There is no one correct template for these activities. Indeed, it has been suggested that the spiral development process itself must be the evolving product of spiral development. These processes can be enriched and transformation accelerated by more exchange of ideas and experiences across organizational boundaries.

I invite your comments and feedback, which should be directed to:

COL (P) Rick Lynch
Assistant Division Commander (Support)
4th Infantry Division
Fort Hood, Texas 76544
ricky.lynch@hood.army.mil

IDA-JAWP
ATTN: Ms. Paula Anselmo
1801 North Beauregard Street
Alexandria, VA 22311-1772
Telephone: 703-845-6846
FAX: 703-845-6810
E-mail: panselmo@ida.org

Ted Gold

Experimentation

Lessons Learned: Commanding a Digital Brigade Combat Team, Rick Lynch, IDA Paper P-3616, June 2001.

US Army and US Marine Corps Interoperability: A Bottom-up Series of Experiments, Rick Lynch, Tom O'Leary, Tom Clemons, and Doug Henderson, IDA Paper P-3537, November 2000.

Experimentation in the Period Between the Two World Wars: Lessons for the Twenty-First Century, Williamson Murray, IDA Document D-2502, October 2000.

Lessons Learned from the First Joint Experiment (J9901), Larry D. Budge and John Fricas, IDA Document D-2496, October 2000.

The Joint Experiment J9901: Attack Operations Against Critical Mobile Targets, Joint Advanced Warfighting Program, September 29, 2000. Prepared for the US Joint Forces Command.

Joint Warfighting Experimentation: Ingredients for Success, James H. Kurtz, IDA Document D-2437, September 2000.

Framework for Joint Experimentation—Transformation's Enabler, Karl Lowe, IDA Document D-2280, January 1999.

Joint Concept Development

Strategic Maneuver, Joseph Sokol, forthcoming, summer 2001.

A Historical Perspective on Effects-Based Operations, Williamson Murray, with Thomas O'Leary, Joel Resnick, Dennis Gleeson, and Gwen Linde, IDA Paper P-3606, forthcoming, June/July 2001.

Taking the Revolution in Military Affairs Downtown: New Approaches to Urban Operations, William J. Hurley, IDA Paper P-3593, forthcoming, summer 2001.

Future Joint Force Headquarters, Scott Schisser, IDA Paper P-3601, forthcoming, June 2001.

Joint Strike Force Operational Concept, Joint Advanced Warfighting Program, IDA Paper P-3578, forthcoming, July 2001.

New Perspectives on Effects-Based Operations: Annotated Briefing, Dennis J. Gleeson, Gwen Linde, Kathleen McGrath, Adrienne Murphy, Williamson Murray, Tom O'Leary, Joel B. Resnick, IDA Document D-2583, June 2001.

Stimulating Breakthrough Change: An Operational Concept for a Future Joint Force, Karl H. Lowe, IDA Paper P-3602, forthcoming, June/July 2001.

War and Urban Terrain in the Twenty-First Century, Williamson Murray, IDA Paper P-3568, November 2000.

Military Operations in Urban Terrain: A Survey of Journal Articles, D. Robert Worley, Alec Wahlman, and Dennis Gleeson, Jr., IDA Document D-2521, October 2000.

Transformation Process

Red Teaming: Shaping the Transformation Process: Annotated Briefing, John Sandoz, IDA Document D-2590, forthcoming, June 2001.

Thinking About Innovation, Williamson Murray, IDA Paper P-3576, forthcoming, June 2001.

Red Teaming: A Means for Transformation, John F. Sandoz, IDA Paper P-3580, January 2001.

Developing Metrics for DoD's Transformation, Joel B. Resnick, IDA Document D-2528, October 2000.

Seminars and Workshop

Workshop on Advanced Technologies for Urban Operations, November 14-15, 2000: Summary of Proceedings, Hurley, William J., IDA Document D-2574, forthcoming, June 2001.

Joint Advanced Warfare Seminar, James H. Kurtz, Daniel E. Moore, and Joel B. Resnick, IDA Document D-2346, July 1999.

Workshop on Advanced Technologies and Future Joint Warfighting, April 8–10, 1999: Summary of Proceedings, William J. Hurley, Phillip Gould, and Nancy P. Licato, IDA Document D-2343, May 1999.

General

FY2000 End of Year Report: Volumes I, II, and III, Theodore S. Gold et al., IDA Paper P-3571, November 2000.

Preface

This paper was prepared for Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics under the task order Joint Advanced Warfighting Programs (JAWP). It addresses the task order objective of generating advanced joint operational concepts and joint experimentation to assist the Department of Defense in attaining the objectives of Joint Vision 2020. Members of the JAWP contributed to the ideas and review of this report.

The JAWP was established at the Institute for Defense Analyses (IDA) by the Office of the Secretary of Defense and the Joint Staff to serve as a catalyst for stimulating innovation and breakthrough change. The JAWP Team is composed of military personnel on joint assignments from each Service as well as civilian analysts from IDA. The JAWP is located principally in Alexandria, Virginia, and includes an office in Norfolk, Virginia, that facilitates coordination with the United States Joint Forces Command.

This paper does not necessarily reflect the views of IDA or the sponsors of the JAWP. Our intent is to stimulate ideas, discussion, and, ultimately, the discovery and innovation that must fuel successful transformation.

Introduction

From April 1997 to April 1999, I had the privilege of commanding the 1st Brigade Combat Team (1BCT), 4th Infantry Division, at Fort Hood, Texas. The 1BCT at that time was engaged in a series of training events and experiments that were focused on the potential application of information technology to military operations. The 1BCT learned many lessons. The purpose of this paper is to share those lessons, and to make recommendations on how to best apply information technology to warfighting.

As we in the US Army work our way into the twenty-first century, we have identified information technology as a critical enabler. We are convinced, intuitively, that the proper employment of information technology will enhance our situational awareness. Ideally, we will have better visibility on where we are, where our buddies are, and where the enemy is.

Across all the Services, great work has been done experimenting with information technology. Some have labeled this as *experiential learning*. We have found that when it comes to working with new technology, we truly learn by doing. We are working our way into uncharted territory: the military applications of information technology. Clearly, we can learn from businesses and industry, and we can postulate the uses of the technology. However, the environment in which the US Army operates is so different than the civilian sector that there are obvious complications.

We owe it to future generations of warfighters to expedite our transition to the battlefield envisioned in the Army Vision. By capitalizing on lessons already learned, and using those as a start point, we can continue to forge ahead. However, a common and accurate phrase to describe our situation is, *we don't know what we don't know*. More poignantly, however, *we don't know what we do know*. We must get better at capturing and disseminating lessons learned.

This paper focuses on sharing lessons learned across all of the imperatives for change—doctrine, organization, training, leader development, materiel, and soldiers (DOTLMS)—though not in the order of the standard acronym. These imperatives provide us with a well-established strategic architecture for planning and executing change. It is important to understand up front, however, that each of DOTLMS imperatives is intertwined—each one is affected by, and affects, the other. The trick is keeping all of these imperatives balanced as we work our way into the future. Each imperative has to be worked, and matured, in concert with the others and not alone.

The tendency seems to be to fixate on the Materiel dimension as we harness new technology. We do that with great risk. Technology isn't the panacea for poor training. People and units must understand the new technology and be able to employ it. Doctrine, tactics, techniques, and procedures (TTP) all must be developed and written, and disseminated and

> Technology isn't the panacea for poor training.

1

understood in order to use the new equipment. *Bottom line: All the imperatives must be worked together—they truly co-evolve.*

> Every experiment was transformed as much as possible into a training event.

The mission of the 1BCT was to be prepared to deploy and conduct military operations and to participate in the Army's experiments, all the while maintaining balanced readiness. In short, we had to be prepared to fight and win our nation's wars, conduct experimentation, and ensure that we provided our soldiers and their families a sound quality of life. Simultaneously managing these three critical missions (warfighting, experimentation, and taking care of soldiers and their families) was a challenge.

During this period the 1BCT participated in many training events, tests, and experiments. Key events included the following:

➤ Task Force Advanced Warfighting Experiment

➤ Division Advanced Warfighting Experiment

➤ Future Battle Command Brigade and Below Limited User Test

➤ Corps Warfighter Exercise

➤ National Training Center (NTC) rotation

Each test and experiment had basically the same hypothesis:

> If we can improve a unit's ability to have situational awareness (Where and I? Where is my buddy? Where is the enemy?), then we will see improvements in lethality, survivability, and the ability to manage the tempo of the battlefield.

A critical point was that every experiment was transformed as much as possible into a training event. Remember, the primary mission of the Brigade Combat Team was to be prepared to deploy and fight to win our nation's wars. We had to be able to conduct experimentation and train simultaneously.

There is clear power in the use of information technology. We can take advantage of improvements in technology to enhance our ability to fight and win our nation's wars.

It is important to always remember in dealing with advanced technology, especially when it comes to warfighting, the Soldier imperative. It is all about the soldiers. We will never replace people on the battlefield. They are the people who make the technology work, and we can never forget that.

Always remember—high-tech demands high touch. Human beings want to be talked to, cared for, taught, encouraged. It was true yesterday; it is true today; and it will be true tomorrow.

Soldiers

The men and women of the US Army are amazing. They are truly the essence of what we do every day. Daily they report for duty, eager to learn, eager to do their very best. All they ask is to be well led and well cared for. They will ensure that we successfully access the power of information technology. Our job, as their leaders, is to ensure we facilitate this process. *Remember: Everything we do is for them, with them.* Improvements in lethality, survivability, and the ability to manage the tempo of the battle will allow us to accomplish our mission, with minimal loss of soldiers' lives. That is what it is all about.

It is important to define early in this discussion the characteristics we want our twenty-first century soldiers to have. To take advantage of the power of advanced technology, specifically information technology, I have found the following characteristics to be highly desirable in our recruits:

> Focused, quick learner

> Comfortable with the technology

> Comfortable in dealing with ambiguous, uncertain situations

> Able to make decisions

> Superb communication skills (orally and in writing)

> Cooperative nature

> Truly embraces change

The next issues to be addressed are:

> How we can attract these kind of people into our Army?

> How we can select soldiers for specific skills and positions?

> How can we retain them?

A critical point to remember that today's soldier is extremely trainable on information technology. Lots of people are concerned how we will teach our junior enlisted the technology. Quite frankly, this is the least of our worries: today's young soldier was most likely taught computers in grade school, and is comfortable on a keyboard and with dealing with electronic information management.

A critical point to remember is that today's soldier is extremely trainable on information technology.

As I walked through the billets in the evenings, I found the majority of our young soldiers had their own personal computers in their rooms. Rather than watching TV or finding ways to get in trouble, a large number of our soldiers spent their free time accessing the Internet, sending e-mail to their family, playing games on a computer. I have been asked, "How is the best way to determine who should be our computer operators? Should we look at General Test (GT) scores, level of college education?" No. The best way to choose your computer operators is simply to walk through the billets at night and find those soldiers who spend their free time working with computers. For example, the best Maneuver Control System (MCS) operator we had in the 1BCT Team had a

GED (General Equivalency Diploma) but he loved computers.

An amazing thing happened as we worked the individual training of our soldiers on the high-tech devices we were given. Routinely, our junior enlisted were given a basic block of instruction on how to use the technology, and then they discovered (by working through the issues) the power of the technology. It was only a matter of time before the soldiers knew more by purely experiential learning about the capabilities of the system than their instructors and their chain of command. These soldiers enjoyed the challenge of how to make the technology work to its maximum potential. Routinely, the young service members became the *center of gravity* on a particular piece of technology, the real experts on a particular system.

Given that our young service members truly have the potential of the technology in their hands, we must empower them to use the technology. A young service member must understand that he is a critical member of the team. He must understand what information the commander needs to make critical decisions and fight the battle—and then be comfortable with approaching the commander, regardless of rank, with that information when it becomes available. This only happens through the establishment of a positive, concerned, caring command climate. Every soldier must feel empowered. They must be convinced that the contribution that they can make to the team is as important, if not more so, than those of the more senior members of the team.

> There is nothing a leader can do in a peacetime environment that is more important than to train our immediate subordinates.

Someone once said, "High tech demands high touch." Service members today, just like those of yesterday, are human beings, complete with needs, desires, emotions, and feelings. Just because we have given the human being powerful computing technology doesn't mean that we can ignore his basic human needs.

We are seeing the phenomenon today of "command by e-mail"—and we are feeling the effects. Sitting in your office, pounding out a message on the keyboard, and pushing SEND aren't communicating. Remember—there is a human being at the other end of the e-mail chain. Did he receive the message? Did he access his e-mail that day? Did he understand what you intended to say? Was he able to perceive, by your use of punctuation, italics, or underlining, what you really thought was important?

Today's service member wants to feel like he is part of the team—part of the solution to the day's problem. He has qualities, characteristics that can contribute to the matter at hand. We must access those abilities. Most importantly, we must work daily to develop our subordinates. There is nothing a leader can do in a peacetime environment that is more important than to train our immediate subordinates.

The critical piece to this training is monthly, written counseling. Whether he admits it or not, every service member wants to be told routinely how he is doing. It is imperative that we sit our subordinates down at least once per month and counsel them in writing. We must devote the time (and it does take time, but it is

time well spent) to articulate in writing our subordinates' strengths, weaknesses, and objectives for the following month. We must—through routine, uninterrupted, focused counseling—tell them how they are doing, and what we want them to do to improve (and just as important, what we are going to do to help them improve.)

We must remember that our subordinate leaders are service members as well and need the same "high touch" that our junior enlisted do. Leaders must also be counseled. In addition, we must provide a mechanism where our leaders (at all levels) can get focused feedback from their subordinates and peers as well as from us, their supervisors.

An issue then develops—*retention*. We train our soldiers on the use of information technology. These soldiers, often through trial and error, learn even more by teaching themselves and sharing lessons learned. The ever-present contractor sees the talent of the young soldier and then convinces him or her to leave the Army, do basically the same job, and dramatically increase his or her salary overnight.

To that end, we must do something now to retain our quality soldiers, especially those with critical, highly technical skills. Soldiers with these skills tend to be low density (there aren't very many of them) but in extremely high demand. We give proficiency pay to our pilots and our doctors. It is time that we recognized the irreplaceable contribution these young soldiers make and reward them accordingly. However, that pay is only part of the solution. There are a variety of things

> **We must do something now to retain our quality soldiers, especially those with critical, highly technical skill.**

that we can do to retain our soldiers not only today but tomorrow as well:

- ➤ We can accelerate their promotions and provide bonuses.

- ➤ We can stabilize them in their current position.

- ➤ We can focus on their families by providing programs for kids, improving child care, and providing adequate on post housing.

- ➤ We can provide employment opportunities for members of their family.

- ➤ We can provide them the opportunity to improve their retirement package (a 401k kind of program).

We must always remember that "adventure sells." The young soldier, and his young leaders, joined the US Army looking for something different than what society had to offer. If he had wanted to be a computer programmer or a telephone technician, he could have chosen to work for Microsoft or AT&T. Our soldier longs for the "intangibles" that life in service to our nation offers, such as the comradery, discipline, and shared hardships. He wants to travel to far-off, exotic places; do things (jump out of airplanes, rappel out of helicopters) that his buddies back home can't do; and then he wants to be able to go home and brag. We must foster this kind of adventurism.

It is imperative that we look closely at what motivates these high-tech warriors, and then nurture it. An impediment to this process is the current "up or out" policy we have in our Army. Many of the soldiers with high-tech skills love doing their job (operating ABCS (Army Battle

Command System) boxes, installing computer networks, etc.) but have no aspiration to be leaders. The idea of being a squad leader or a platoon sergeant isn't appealing to them. In fact, in many cases, it scares them to death. Given the choice to attend the Primary Leadership Development Course or leave the service, many chose to leave. We need to revisit this policy.

We must look closely at our personnel assignment policies. First, we must ensure that we utilize the talents of our service members after they have been in a digital organization. Routinely, we are sending them to units that don't have digital equipment. Information technology skills are so perishable that it is only a matter of months before the soldier has forgotten all that he was taught. Worse yet, he did not have the opportunity to train his fellow soldiers on what he did know. He didn't share what he had learned before he changed assignments.

Stabilization isn't the answer. Stabilizing a small cadre of individuals and let them work digitization solely doesn't do the rest of our services any good. Give a soldier three years in a digital outfit, and then assign him to a place where he can either teach his skills to others or else document his lessons learned.

Stabilization has a bad side effect, creating over time a "have and have-not" hierarchy within our Army. Some soldiers will always be assigned where the high-tech equipment is, and others will never see it. That is wrong. We must continue to rotate our soldiers through all different types of units. This increases our experi-

> Information technology hasn't yet (and probably won't ever) actually destroy the enemy on the battlefield.

ence base across the force, and gets everyone to "buy in" to the power of information technology. Reading about how well information technology works doesn't give you the same sense of ownership as being in a unit that has it, with you personally benefiting by the power of the technology.

We must look at how we are training our officers and non-commissioned officers (NCOs). We need fewer specialists, and more generalists, in our command posts. Routinely, the battle captain was not able to access artillery or intelligence systems: we had trained him to be an operator. Service members on tomorrow's battlefield must truly be multifunctional and multidisciplined. They must be able to understand a wide range of issues and not be limited to some stovepipe operation.

This, however, is a slippery slope to a dangerous situation: information technology hasn't yet (and probably won't ever) actually destroy the enemy on the battlefield. Lethal platoons and company teams still have to be maneuvered to bring combat power to bear on the enemy. As a result of that, we still must have young officers and NCOs who are extremely proficient in a particular set of skills *before* we try to develop them into multifunctional soldiers. Soldiers must always be grounded in the basics.

There is also a move to get our NCO corps doing, over time, more of the particular tasks that we expect of our officer corps today. To that I say great—but! Someone has to take care of the "sergeant's business." Someone has to supervise motor pool operations; check TA50;

lead physical training; and teach, coach, and mentor our junior enlisted. In the 1BCT, we were blessed with a top-notched set of NCOs. They truly took care of the sergeant's business. They focused on individual and collective training up to and including crew level. They deployed the 1BCT, ran ranges, and ensured our soldiers and equipment were prepared for deployment and combat operations. Someone has to do the sergeant's business in the twenty-first century.

Leader development will be dealt with in detail in a subsequent chapter, but it is important to discuss *individual soldier development*. We must first focus on the basics in both individual and collective training. For the majority of soldiers, we must not change what we currently teach in basic training. Teach them to be soldiers first before we worry about teaching them to operate high-tech equipment. We found that NCOs, having been trained as Instructor Key Personnel by qualified personnel, were able to train new soldiers on the basic use of equipment in a relatively short period of time.

For the critical, low-density–high-demand MOSs (military occupational specialties), we must change our institutional learning base to give the soldiers the skills, knowledge, and attributes (SKAs) they need to perform once they reach their first unit. Significant time must be spend early in their development to teach them maintenance and repair procedures for the high-tech equipment.

We must ascertain the best way to continue the education of our critical specialists. Moore's Law states that information technology changes every 18 months or so. Consequently, we must have a system to return our soldiers to a training base (government, contractor, or academic) to keep him abreast with the most recent advances in the technology. In addition, we must provide incentives for self-development. Given certain incentives, soldiers will want to improve their capabilities.

To create an environment where soldiers can flourish, we must create and sustain a real learning environment. As leaders, we must acknowledge that "We don't know what we don't know" as we work our way into the future. We must embrace change, continually search for better ways to use the new technology, and be receptive to good ideas bubbling up from the privates and specialists. Given this environment, the young soldier will improve or hone his special skills, so he can have a greater impact on his unit performance.

It's all about the people. They make the difference, they access the power of the technology, they make things happen. We must first acknowledge all of this, and then align our priorities to ensure we are doing the right things for the people. All else will follow.

Leader Development

The most important thing we can do today to improve our capabilities on tomorrow's battlefield is to focus on leader development. We must identify what skills, knowledge, and attributes we need in our Force XXI leaders:

- First, it must be emphasized that the majority of the attributes we need in tomorrow's leaders are the same as those we have needed in yesterday's and today's.

- Leaders must be concerned, caring, and compassionate. They must truly care for soldiers and their families.

- They must be technically and tactically proficient.

- Leaders must also be able to communicate their thoughts and ideas effectively. Leaders also must be effective teachers, coaches, and mentors.

- Most importantly, leaders must epitomize Army values. They must live by example the values of duty, honor, integrity, selfless service, respect, loyalty, and personal courage. They must "walk the walk, not just talk the talk." Everything they do, every day, must reflect positive personal commitment to Army values. In turn, they must ensure that their subordinates live Army values.

Given information age technology, there are certain traits that our leaders must have to truly capitalize on the capabilities resident in the technology. Leaders must clearly be comfortable with advanced technology—they cannot be intimidated by computers. They must be more than conversant in technical terms—they must master the technology.

Leaders on tomorrow's battlefields must be able to foresee options and impacts in a complex setting. They must be decisive. They must be comfortable in uncertain, ambiguous settings. They must be able to recognize the second- and third-order effects of decisions they make. They must be focused and quick learners.

> In a setting where abundant amounts of information are available, leaders must be empowered and decentralized.

In a setting where abundant amounts of information are available, leaders of the US Army must be empowered and decentralized. As a commander of a digital brigade combat team, I had visibility on the location of each and every vehicle in the 1BCT. For example, I could focus in on the actions of D32—the wingman tank of the 3rd platoon, Delta Company, 3-66 Armor. Then, if I chose to, I could have told D32 where to go and what to do—totally circumventing three layers of the chain of command. But I chose not to do that. I set the filters on my digital equipment to show me company-level icons. I, as a 1BCT Commander, fought companies. Battalion commanders fought platoons, company commanders fought individual platforms—this has not changed. However, there are individuals who, given the opportunity to micromanage their units, will do so. This will

have a disastrous effect on subordinate leadership.

One example of allowing technology to get in the way of effective leadership is the phenomenon of managing by e-mail. Some leaders, given the ability to communicate their thoughts and ideas electronically across wide formations, will do that via e-mail. When that happens, there are two results:

> The subordinate leaders feel that they are being bypassed.

> The recipient of the e-mail doesn't enjoy the sensation that the human dimension of face-to-face communication gives us. We must ensure that we select and then develop leaders who emphasize the human dimension of what we do. Remember—high tech demands high touch.

The selection of leaders is critical, especially at the more senior level. The most effective leader development program will only be as good as the basic qualities of those leaders we select.

At the Department of the Army level, we currently rely on input only from the superior in the selection process for senior leaders. Battalion and brigade commanders, and general officers are selected based solely on what their bosses wrote on their officer efficiency report (OER). Usually the bosses know that the mission was accomplished, but rarely do they know *how* the mission was accomplished. Was the subordinate leader abusive? Did he ride

> Operations on tomorrow's battlefield will be 10% planning and 90% execution, and will be very command centric.

his subordinates to the point of breaking? Did he step on his peers to accomplish the mission? This current system doesn't give us a total look at the past performance and potential capabilities of future leaders. There must be a better way of selecting leaders.

In the 1BCT, we worked with Fort Leavenworth to utilize a 360-degree assessment program. After the NTC rotation, peers and subordinates were surveyed as to what they thought of their boss, focusing on attributes we want in our leaders. For example, one question was "How do you think your boss did during the intense, stressful environment of the NTC?" This information was then given back to the soldier being evaluated, concentrating on identified strengths and weaknesses, for his own professional development. Throughout the 1BCT, leaders who were given 360-feedback found the program to be very useful. Eventually, we as an Army could carry that one step further, and design a system that allows selection boards and other mechanisms to take advantage of this information.

Operations on tomorrow's battlefield will be 10% planning and 90% execution, and will be very commander centric. It will be up to commanders at all levels to make the right decision, at the right time, to truly take advantage of information technology and improve our lethality, survivability, and ability to manage the tempo of the battlefield.

9

A commander must be decisive. He must be able to make decisions in situations where he may not have all necessary information. He must define for himself, early on, what decisions he will have to make and when. The commander must be able to personally craft and then carefully articulate those pieces of information he must have to make decisions. These information requirements still take the form of EEFIs (Essential Elements of Friendly Information) and PIRs (Priority Information Requirements). Given the insertion of information technology, these information requirements have become very important. At the same time, it is extremely easy to become overwhelmed by information. Information requirements, dictated by the commander, help us refine information to those discrete pieces of what the commander needs to know.

Information requirements are dynamic and constantly changing. The commander must be able to continuously evaluate his information requirements to ensure he is asking the right questions. The staff must also monitor the situation and tell the commander, almost continuously, which of the information requirements have been answered, and which are still unknown. They must also routinely make recommendations for changing information requirements (adding a new one, modifying an existing one, or deleting one) to the commander.

A commander must have a vision. Based on his own mission analysis, he must be able to see, in his mind's eye, what the desired outcome of the battle is. Then he must be able to formulate, in conjunction

> The counseling must focus on strengths, weaknesses, and objectives for the following month—truly the essence of leader development.

with his staff, a concept of the operation that might work. He must personally craft and articulate his intent for the operation. This isn't a new concept peculiar to tomorrow's battlefield. Currently, we don't do this very well. In a recent study performed at the US Army's NTC, data indicates that subordinates only truly understand their higher commander's intent 34% of the time.

The commander must be able to think like the enemy:

▶ What are the enemy's options?

▶ What decisions must he make and when?

▶ What are his vulnerabilities?

▶ What are his capabilities?

Now that I have defined what a leader must be able to do, how, when, and where should we as an Army develop these attributes? In accordance with our training doctrine, leader development occurs at many places: at the institutional level (e.g., advanced courses, command and general staff college), at the unit level, and by self-development.

Leader development at the institutional level

At the institution level, we must empower our leaders with the skills necessary to perform rudimentary operations on the equipment that will be present in their unit when they arrive. We have always expected our leaders to be technically proficient. This is even more pronounced in those units that have high technology equipment. We do our leaders a disservice

by assigning them to units in which the young privates know more about the equipment than they do.

> The leader must be continually placed in a stressful, demanding situation, and then evaluated on his response.

Above and beyond rudimentary knowledge of the equipment, we must teach our leaders at the institution how to utilize all of the equipment in an integrated fashion. We must focus on the issue of *information sharing* and *integration*.

We must develop a system to teach leaders the art and science of battle command. The idea of being flexible, adaptive, able to "think on your feet" is something that can be matured in a institutional training environment before the leader reports to his unit.

Leader development at the organizational level

At the organizational level, there are several in-house techniques that units can use to focus on leader development. Most importantly, monthly written counseling of every single individual in the organization is critical. The counseling must focus on strengths, weaknesses, and objectives for the following month—truly the essence of leader development. The most important thing that anyone does in a peacetime Army is training his immediate subordinate. As we all know, a critical part of that training is evaluation. We must tell our subordinates how they are doing as leaders, and recommend ways they can improve. This is done through repetitive counseling session in which the good, the bad, and the ugly are discussed.

At the end of each counseling session, ask the question "How am I doing?" This will be an excellent venue for feedback from subordinates.

As with training of muscles, training of leaders must be exhaustive. That is the only way the leader is going to grow, to develop into a better leader. The leader must be continually placed in a stressful, demanding situation, and then evaluated on his response. Training events must focus on placing leaders at all levels in stressful, complex situations. They must routinely be forced to deal with uncertainty.

Time is the most critical resource when it comes to leader development. To free up time for leader development, we must permit our NCOs to do their job. Let sergeants do the "sergeant's business"; this will free up the officers to concentrate on leader development training.

And we must make time for the NCOs to train the junior NCOs. A technique that we used in the 1BCT was to release all of the junior enlisted (SP4 and below) at 1600 hours daily. This accomplished a variety of things—all good. It got the young enlisted home at a reasonable hour every day. This was much appreciated by the youngsters and their families. They had a predictable duty day. They knew that they had to come to PT (physical training) at 0630 every morning, and they knew that they were going to be released at 1600 every day.

More importantly, the time from 1600–1800 every day gave the Command Sergeant Major (CSMs) and 1SGs time to train their junior NCOs. They could use that time for daily NCO Professional Development to rehearse classes, or to give the young NCOs time to prepare for the next day's events.

11

Training has always been, and always will be, the cornerstone of our readiness program. Nothing on the digital battlefield will preclude the need for tough, demanding, realistic training at both the individual and collective training level. Always remember—technology isn't the panacea for poor training. Soldiers and units will perform in combat exactly how we had trained them to perform in our peacetime training. As a result, we must always make training "Job One."

Regardless of whether you are training individuals or teams, you must first train the soldiers in the basics, the blocking and tackling. This will never change. Soldiers and their units must be grounded in the basics. They must understand their people, their equipment, their standing operating procedures (SOPs)—everything that we have always reinforced in training. We still must teach our individual soldiers the common skills that will keep them alive in combat. Platoons and company/teams must still be able to move with authority (in and out of contact), take actions on contact, hit what they shoot at, report accurately, and mark and bypass obstacles.

Once we are convinced that our soldiers and units are proficient in the basics, then we can turn our attention to the new technology. We must first spend time teaching the technology—what it does, how it operates, how it is repaired, etc.

> Once we are convinced that our soldiers and units are proficient in the basics, then we can turn our attention to the new technology.

We must understand in detail the capabilities of the systems.

After everyone on the team understands the technology in detail, then the training program must shift its focus to take advantage of the technology, with the focus on the application of the technology to basic skills. Proper utilization of information technology should improve our lethality, survivability, and ability to manage the tempo of the battlefield, but this will only occur if we have trained our individuals and units to apply this technology to already existing basic skills.

Battle staff training is an extremely complex and demanding piece of the digital training puzzle. Battle staffs exist at all levels, from company to corps. They are where information is fused and integrated. Battle staffs take available information, apply it against information requirements the commander has articulated, and present the information to the commander when he needs it and in the format he desires. We have always expected our battle staffs to be able to (1) produce an order in a timely fashion that might work, (2) track the battle, and (3) make recommendations to the commander. But while these collective skills are still critical, they aren't sufficient enough to capture the power of information technology.

On the digital battlefield of tomorrow, we must have the hyper-proficient staffs who understand what's required of them as

individual staff members, but, more importantly, what's required of them as a member of an integrated staff. They must work together continuously, and this doesn't happen accidentally—it is a result of a detailed battle staff training program.

> A major issue is how to forge high performance units that are task organized just prior to the execution of a complex mission.

Battle staff training must happen routinely, and probably as frequently as once a week. The commander must be involved in the battle staff training. He must lead the staff through mission analysis. He must personally craft and carefully articulate his commander's intent for the operation. He must detail information requirements, both friendly and enemy, to his staff. He must work with the staff on a detailed wargame of the operation. He must lead them through a series of potential branches and sequels based on the enemy doing something unexpected.

The battle staff training should be focused on specific vignettes that force the staff to use all of the available systems to access and integrate information. Logical vignettes, based on experience at NTC, would include battlespace management, response to enemy air attack, movement control, and penetration box operations.

The major difficulty with battle staff training is the overhead required to plan, conduct, and "after-action review" (AAR) the training event. We must develop a low-overhead driver for digital battle staff training. Simply put, this would be a training location (a battle staff conduct of fire trainer, if you will) where the commander could take his staff, turn on a switch, and conduct training. Some simulation must be connected to the ABCS boxes to cause information to be populated to the various systems. Battle staff training could then focus on the acquisition of that information, the integration of the information, and the presentation of the information to the commander.

In line with the low overhead driver, we must have a digital AAR capability. After the battle staff training session, we must be able to "go back in time" and see what information was available when (and where) as part of the AAR. Snapshots of all the boxes must be available (what was the operator on screen "X" looking at time "Y") for the AAR.

This is truly a team sport. Building the team, and accepting new people onto the team as quickly as possible, is a difficult training challenge. The staff and subordinate commanders must think like the commander, to reach a point in their relationship where they can actually anticipate what he is going to say next. Commanders must spend time with their subordinates, routinely telling them what they are thinking and why. And this time must be spent in a variety of settings: social, garrison, and, most importantly, in tough, demanding training exercises.

Teams come in many fashions in units (digital or analog): *standing teams* (like established battle staffs), *ad hoc teams* (targeting teams), and *informal teams*. To make these teams as effective as they can possibly be, tough, demanding training is essential. If we expect the team to work well together in a stressful, demanding situation, we must make the training replicate that. The key in each situation is to

routinely subject the team to situations that cause them to bond.

All training must include a non-cooperative, thinking, adaptive enemy. We cannot allow commanders to control both the friendly and enemy forces in training events. That is just too easy. There must always be an opposing force (OPFOR) commander whose primary purpose is to defeat your unit, to cause you to do something that you did not want to do. In all training exercises, there must be an OPFOR who is continually looking to concentrate his strengths against your weaknesses.

All training must be evaluated. We must develop a core of "digital OCs" (observers/controllers) who have had personal experience in developing, training, and fighting with digital systems. These digital OCs must be present to help commanders develop their training programs, and to evaluate training as it is conducted. They must be there to facilitate AARs, and to capture lessons learned and feed them back into the next training cycle.

A major issue is how to forge high performance units that are task organized just prior to the execution of a complex mission. In other words, how do you facilitate the bonding of the new element with the rest of the organization? A major solution to that particular problem is standardization. Such things as TACSOPs (tactical standing operating procedures), in particular, need to be standardized. This can also be facilitated by early identification of potential missions. This allows the commanders to establish personal contact (either by e-mail, video-teleconferencing, or personal visits.)

A key element in training digital organizations is ensuring that all subordinates have confidence in the technology. If commanders and staffs are hesitant to use the technology because they believe it is unreliable or inefficient, then they will not train on it. Information that appears on the screen must be taken at face value and not second-guessed. This can only be accomplished by repetitive, properly resourced training events in which the technology is used. Confidence in the technology can only be attained by using it routinely with good results.

Digital skills are extremely perishable. If soldiers (and leaders) don't use the technology on a routine basis, they will lose the needed skills. We must make an effort to provide a garrison capability for day-to-day digital operations. For example, we should put the ABCSs in all headquarters (corps through battalion), and use these systems for day-to-day operations (passing taskings, e-mail communication, etc.). In addition, we should put FBCB2 (Force XXI Battle Command Battalion/Brigade and Below) in company orderly rooms and require that FBCB2 be used in place of e-mail. This will provide for operator sustainment training.

We must ensure that in our training programs we are always conscious of the fact that we will have a combination of digital and analog units in our formation. During the March 1999 NTC rotation, the 1BCT included an analog light infantry battalion out of Hawaii as well as a National Guard Aviation unit. This will always be the case—so we must prepare for this in our training programs. Establishing properly equipped, properly trained digital liaison officer (LNO) teams can facilitate this. Most importantly, battle staffs must be

prepared to disseminate plans and orders both digitally (over ABCSs for example) and by analog means (good old-fashion acetate and grease pencils).

The bottom line: We as an Army can take advantage of information technology now with a good, detailed, well-resourced training program. There is "goodness" in the technology as it currently exists. We can access this goodness by training our soldiers and our units on how to leverage that technology.

Now the issue becomes, how do you fight with this new organization, empowered by information technology? This is clearly a challenge in view of "we don't know what we don't know." We can hypothesize that "maybe we would fight like this" but we find that our thoughts generated while working in an air-conditioned office don't work when applied in the field. Specifically, what's the doctrine, what are the TTPs that will allow us to capitalize on this advanced technology?

Spiral development here is essential:

> Get the technology in the hands of the user as soon as possible.

> Give the user some generic concept, a starting point, on how to fight with these new systems. And then turn him loose.

> Watch carefully what he does.

> Focus on what worked, and what didn't.

> Then take these ideas back into the doctrine-writing business to refine the concept.

The key piece is developing a system where these lessons learned are captured and institutionalized. Routinely at Fort Hood we were too busy to stop and codify what we did—we simply moved on to the next major event. Someone at the institutional level must capture lessons learned and disseminate them across the force.

> **First, it is critical that leaders who intend to use the technology trust the technology.**

We must continue thinking "out of the box." Information technology properly applied does indeed increases our lethality, our survivability, and our ability to manage the tempo of the battle. As difficult as it is, we must ensure that our thought processes aren't hamstrung by "the way we used to do business." Routinely, the 1BCT would be given a new piece of "kit" along with someone's ideas of how to best use it. After just a couple of iterations, we soon found ourselves using the kit totally different than it was originally intended. Allow me to take some time to share some lessons learned on "how to fight" with information technology.

First, it is critical that leaders who intend to use the technology trust the technology. To make sound tactical decisions in a timely fashion, you must believe that the icon you see on the screen truly represents the location of the friendly or enemy unit identified. If you spend time questioning the technology, or hesitate to make a decision based on the fact that you don't trust the technology, you have already degraded its potential to help you fight.

Battlespace has indeed increased—as well it should have. The normal battlespace for a 1BCT using information technology is 30 to 45 kilometers wide and 40 to 60 kilometers deep (about three times what the 1BCT used to control). That's good stuff—gives us plenty of room to maneuver. We have the ability to expand our

battlespace directly as a result of our increased situational awareness. If we know where we are, and where all of our friendly forces are, we can disperse our forces over a wider area and then concentrate them at the right place, at the right time, to kill the enemy.

> The communications backbone to support your operation must be planned first. Given the terrain in the area of operations, where do you need to position your communication assets to provide yourself with the ability to communicate?

This is a key point: When we say that information technology allows us to manage the tempo of the battle, this doesn't imply that we do everything faster. It means that given situational understanding across the force, we can choose to engage the enemy at the time and place of our choosing, and at conditions that are to our advantage—not his.

Given the expanded battlespace, the key element is first answering three questions:

➤ How do I communicate over these large distances?

➤ How can I sustain myself over these large distances?

➤ How do I protect key high-value assets (HVAs) throughout my battlespace?

Answers to these questions will enable you do determine what's feasible, given current conditions. Think about the enemy's intentions, capabilities, and vulnerabilities. Then—and only then—should you start developing a maneuver plan to support your concept of the operation.

How do I communicate over large distances?

Communicating over expanded distances is hard. It is hard when you are trying to transmit only voice. It is even more difficult when you are trying to transmit digi-

tal information. The communications back-bone to support your operation must be planned first. Given the terrain in the area of operations, where do you need to position your communication assets to provide yourself with the ability to communicate?

The digital 1BCT uses many means of communication to transmit information. Single Channel Ground and Airborne Radio System (SINCGARS), Enhanced Position Location Reporting System (EPLRS), Mobile Subscriber Equipment (MSE), and Near Term Digital Radios (NTDR) are all critical, and must be planned for. Once planned for, they must be positioned and protected.

How can I sustain myself over large distances?

The next issue, given the expanded battle-space of the digital brigade combat team, is sustainment. The Conservative Heavy Design for our divisions has redistributed the majority of Combat Service Support (CSS) to the Forward Support Battalion (FSB). Maneuver battalions no longer have internal mechanics, fuelers, ammo transport vehicles, or cooks. All of these assets reside in the FSB. Forward Support Companies (FSCs) are formed to support each of the maneuver task forces.

This design demands careful planning on the part of everyone on the team. The maneuver task force commander must maneuver his FSC just as he does his maneuver companies. He must plan for the proper positioning of logistics assets throughout his battlespace, and once

17

again plan on how he is going to protect those assets. He no longer has the latitude to "hand wave" the logistics planning to support his operation. He must make planning for resupply a priority. Because he no longer directly controls his mechanics, his fuelers, and his ammo vehicles, he must plan for the proper linkup of CSS assets with maneuver assets at the right place, at the right time. Difficult but critical stuff.

> You must pick up the red pen first. You must think like the enemy. What's he trying to do? What are his capabilities, vulnerabilities, and intentions?

How do I protect key HVAs throughout my battlespace?

The next major consideration on the part of the commander of the digital 1BCT is how is he going to protect all of his HVAs over this expanded battlespace. Because elements are now widely dispersed over a sector 30 kms in width, how do you ensure that your HVAs are protected. Ask yourself:

➤ What are your capabilities, vulnerabilities, and intentions?

➤ What assets are so critical to your operation that if you lose them, your chances of victory are severely degraded?

These assets become your HVAs, and you must protect them. In addition, the Division Commander may have placed some of his HVAs in your sector, and you must protect them as well. Examples of HVAs include counterfire radars (Q36, Q37), critical intelligence assets, artillery units, logistics elements, and air defense radars (Sentinels). You must make planning for their protection a priority.

You must pick up the red pen first. You must think like the enemy. What's he trying to do? What are his capabilities, vulnerabilities, and intentions?

Too many times we allow the intelligence officers to develop what they believe to be the "most likely enemy course of action" and we develop our concept of operations against that enemy plan. We don't take the time to step away from the map board and think:

➤ What does the enemy want to do?

➤ What's the correlation of forces between what he has and what I have?

➤ What's he going to try and strip away from me?

Thinking like the enemy drives all subsequent activity. Primarily it drives development of PIRs, those things that we must know about the enemy so we can kill him. These PIRs, in turn, drive positioning of assets to cover named areas of interest (NAIs).

As mentioned before, fighting on the digital battlefield is 10% planning and 90% execution. We must retain flexibility and agility to take advantage of the improved lethality, survivability, and ability to manage the tempo of the battle provided to us by information technology. Too many times we develop a plan (again based on what the S2 tells us in the most likely enemy course of action), and then we fight that plan, regardless of what the enemy is actually doing. All wrong! That isn't to say we shouldn't waste our time developing a plan. We must continue to do that. We just must acknowledge that the enemy is probably doing something

different than we antici-pate, so we must remain flexible. Our planning staffs should spend a large portion of their time de-veloping branches and sequels to our original plan, the "What if's." What if the enemy does this—then we'll do that. And on and on. Planning never stops. It is eas-ier to issue a frag order off of a plan if that frag order was developed before the bullets started flying.

Collaborative planning tools are absolutely essential in planning simultaneous, complex operations.

We must continue to develop the para-digm of "See them deep—kill them deep." Ideally, the only direct fire en-gagements we will have will be with their supply convoys. This is the true advan-tage of information technology, killing the enemy before he gets to friendly forces. Using JSTARS (Joint Surveillance Target Attack Radar System), unmanned aerial vehicles (UAVs), Army aviation, Multiple-Launch Rocket System (MLRS), and can-non artillery—combined with a maneuver force that positions and protects HVAs and fixes the enemy force—is an effective way of fighting. We must work to place our sensors (ground and air, electronic, manned, unmanned) as deep as possible.

Remember, we have a wide variety of sensors at our disposal. Ground recon-naissance assets are essential to our opera-tion. However, if you put all your eggs in some "high-tech basket" (like JSTARS or UAVs), and that technology fails right when you need it, you are out of luck! You are now dispersed over a wide area with no idea where the enemy is. He can attack you one piece at a time and destroy your forces at his leisure. He now has the advantage.

Under the Conservative Heavy Design, each ma-neuver brigade had its own recon troop. This Brigade Recon Troop (BRT) proved to be the most reliable, the most dependable, and the most flexible reconnaissance asset at my disposal. Proper initial positioning is critical. Put your recon troop where you believe the enemy is coming, based on having "thought like the enemy." Position NAIs in areas where the enemy must travel through, and then position recon troop assets to cover these NAIs. Importantly, place a Targeted Area of Interest (TAI) in proximity to the NAI covered by the re-con troop. Knowing where the enemy is only part of the equation. Killing him is what it is all about. Because your recon troop has been able to find the enemy, a TAI allows for an efficient method to kill him. Plan fires (rocket, artillery, and at-tack aviation) on that TAI, and work the sensor-to-shooter link very hard in re-hearsals.

A drill that we developed in III Corps that worked very well (given improved situational awareness and understanding) is called "pen-box operations." We can use pen-box operations to defeat the en-emy at any point of penetration, regard-less whether it is a minefield breach, a river-crossing operation, or anything that causes us to channel our forces through a concentrated area.

The TTPs are relatively simple, all based on three phases of fire (which I will de-scribe in a moment). Once a determina-tion is made as to where the penetration will take place (utilizing all forms of re-connaissance assets available), the zone of penetration is determined. This is defined

as the zone around the point of penetration in which enemy forces can influence our operation.

During Phase I fires, we first kill all enemy artillery (and observers) that is within range of our zone of penetration. This is a significant effort—it takes a lot of time and effort (and resources) to accomplish this phase of the operation, but it is worth the time. Sure beats having enemy artillery rain down on you right when you have massed your forces at the point of penetration.

During Phase II fires, we kill those enemy forces that can be used to counterattack us at the point of penetration, specifically those that are within the zone. This is pure planning calculus, given the position of our forces and the enemy counterattack forces, and deciding which ones can indeed influence our operation. We must reach out and attrit them during Phase II.

During Phase III fires, we will destroy those forces at the point of penetration. Then, and only then, do we move maneuver force through the penetration. Protect the force !

We can use JSTARS to queue the UAV. We found that routinely the UAV can give us targetable data. A decision has to be made early in the process whether we want to use our limited number of UAVs as a reconnaissance tool or as a targeting tool. In addition, there is a tendency to want the UAV to loiter in order to assess Battle Damage Assessment.

In the Division Advanced Warfighting Experiment, we had ground sensors, called Raptors, which were basically smart minefields with seismic and acoustic sensors. The same issue occurred as with the

> The moral of the story is, you must always have an analog backup to your digital operations.

proper use of UAVs. We had to decide when to transition the Raptor from a set of "eyes" to a killing system.

We found collaborative planning tools to be absolutely essential in planning simultaneous, complex operations. The key is getting to the point when all commanders have the same "understanding" as to what's happening on the battlefield. This can only be accomplished by routine commander-to-commander dialogues. In the Division, we used collaborative planning tools extensively.

Routinely throughout the course of a fight, the Division staff would announce the Date-Time Group (DTG) of the next collaborative planning session. At the same time, the staff would announce what piece of the fight (what terrain, what degree of resolution, what graphical control measures, etc.) we would be looking at. Staffs at all levels would work to ensure that a common operational picture was presented to commanders. At the designated time, the Division Commander would come on the collaborative planning net, and describe his view as to what was happening (both friendly and enemy operations, constraints and restrictions, etc.). He would use a "John Madden pen" to write on the screen, over the top of the posted map. Simultaneously, all of these subordinate commanders could hear the Division Commander's voice and see what he was writing on the screen. Then, in turn, each of the subordinate commanders would describe their piece of the fight, using their appointed color pen to highlight specific pieces of the operation. At the end of each session, the Division Commander would review the

session and highlight for us all what he envisioned happening next.

All told, these collaborative planning sessions took about 30 minutes, but they took the place of hours of planning in the analog fashion. We all left these collaborative planning sessions with a common knowledge (and understanding) of current and future operations—a phenomenal capability.

It is essential that in fighting on a digital battlefield, you always maintain a reserve. I had one at the 1BCT level, and the Task Force Commanders created one at their level as well. You will never have perfect situational awareness. There will be enemy forces in your sector that you don't know about. The enemy will do something that you didn't expect. As a result of those unknowns, you must create something that will give you the ability to respond to the unexpected—a reserve.

Creating reserves under the Conservative Heavy Design is complicated, given the fact that each maneuver battalion only has three maneuver companies. And remember—you have already allocated some of your maneuver elements to protect HVAs, again making generating a reserve more complicated. More complicated but extremely essential.

At the 1BCT level, I always kept a two-company task force in reserve. I would identify the main effort, and weigh that main effort with additional assets (intel, fires, and maneuver). Normally the main effort Task Force had four company teams.

At the Task Force level, maneuver commanders tried a variety of techniques to create a reserve element. The most successful was taking the Headquarters Company Commander and making him the commander of a reserve force. Based on the situation, take maneuver platoons away from the lead company teams and give them to the reserve. In this way it was possible to create a fourth maneuver element (the Task Force reserve) that had one or two platoons attached. Very effective.

Finally, always remember Murphy's Law as it applies to advanced technology. All of these great information technology assets that we are developing are exciting and will be very useful on the battlefield. In the 1BCT, we developed our own view of advanced technology: "It's not IF the technology will fail you, but WHEN." You have to be prepared for the technology to fail you at the worst possible time: power sources go away, screens fail, soldiers plug in the wrong wire to the wrong outlet and the box stops working.

The moral of the story is, you must always have an analog backup to your digital operations. For example, a total reliance on aerial reconnaissance is riddled with potential disaster. During our NTC rotation, JSTARS was pulled to a more critical mission, UAV wings froze up, and other support disappeared. When I needed the aerial reconnaissance, it wasn't available.

Organization

The key is organizing around information—not around functions. We can change organizational structure (in the Tactical Operations Center (TOC), or in units themselves) relatively easily, but the change must be focused on facilitating information flow. We must evaluate what inputs come into the organization (what medium, what format, etc.) and what outputs do we expect (orders, graphics, etc.). Once we know that, we can organize our TOCs, headquarters, etc., to truly capitalize on the power of information technology.

A perfect example is plans and operations at the brigade or division level. Routinely, we separate the two functions. However, there isn't an efficient method to ensure that everything the current operations people know about what's happening is transferred to the planning people, or vice versa.

Another example is the information available in each of the ABCS boxes. Routinely, a piece of information that the S3 needed would be resident in the Fire Support Officers "box" but the Fire Support Officer (FSO) never bothered to tell the S3.

There is a tendency to want to reorganize sooner (rather than later) to take advantage of the opportunities that advanced technology provides, such as increased efficiency or new way of doing business. There is a major problem with this line of thought. Reorganizing based on the projected presence of enablers—before the enablers are actually present—is dangerous. There are cost savings (time, people) embedded in the goodness of advanced technology, but reorganizing before that technology is present causes problems in the ranks. It simply just makes things harder.

> Reorganizing based on the projected presence of enablers—before the enablers are actually present—is dangerous.

Thought processes hinder attempts at organizational changes. Many of us are wedded to a specific idea only because we are comfortable with that particular idea. We cannot allow ourselves to be hamstrung by the way things were.

Each of the imperatives is intertwined with each other. Nothing illustrates that example more that the tie between leader development and organizations. If or when we reorganize, we reduce the number of positions that allow our subordinates to grow, then by definition we are affecting our leader development. Nothing takes the place of learning by doing.

Materiel

It is important to first discuss the degree to which changes in materiel affect all of the other imperatives. They are all intertwined. The key to successful transformation lies in the co-evolution of doctrine, training, leader development, soldiers, organizations and materiel. Successful transformation isn't just about materiel.

There are believers in simple fixes: give a unit a new piece of kit, a new "widget" that will solve a problem in this particular area. The new piece of kit supposedly will become the panacea for poor training, poor leader development, etc. All wrong! That new widget now affects everything the unit does.

First, soldiers and leaders must be comfortable with the widget. They have to understand its capabilities and limitations. They have to know how to employ it, how to fix it, how to sustain it. This can only be accomplished by a detailed individual soldier and leader development program.

Next, leaders having a basic understanding of the technology must be able to develop a plan to train individuals and units on how to employ, fix, and sustain the widget. This training will be in addition to all the other training the unit already must perform to maintain its combat readiness. These requirements didn't go away because the new widget appeared.

The unit's organizational structure must be revisited. Will modifications in current organizational design do a better job of employing this new widget? And if the

> It is imperative that we design systems that are interoperable.

decision is yes? Then we must modify organizations, which is a major effort. Soldiers have to move, perform the "duffle bag drag," if you will. Equipment has to be moved, inventoried, and stored. Efficiency reports must be completed.

Once the unit has had an opportunity to use the new widget, changes in doctrine and TTPs will become evident and will need to be captured and institutionalized. SOPs will have to be revisited. As we learn to effectively use new widgets, we truly "learn by doing." Much of the evolution of doctrine and TTPs is trial and error: what worked and what didn't?

As we develop systems, or improve the ones we currently have, we must focus on the integration of their capabilities. Developing stand-alone, stovepiped systems isn't useful. A perfect example is the current lack of integration of the ABCS. Every one of the boxes has some piece of information that the commander needs. The problem is, these boxes aren't integrated: all integration has to take place in the minds of the staff officers or in the mind of the commander himself. Just as important is the seamless integration of FBCB2 with the ABCSs. For example, Blue information that is resident in FBCB2 must be ported automatically to MCS. This will enhance the credibility of the Blue icon. Red information, generated by FBCB2 spot reports, must automatically populate All Source Analysis System (ASAS). Next, ASAS populates MCS with Red icons and now we have what the

commander needs—an integrated Red-Blue picture.

We have acknowledged that we as an Army will fight on a joint and combined battlefield. Therefore, it is imperative that we design systems that are interoperable. For example, the Marine Corps has its own set of digital command and control devices, all different than those of the Army. The only "box" that is the same is the Advanced Field Artillery Tactical Data System (AFATDS) box. The intel box, the operations box, the air defense box, and the combat service support box are all different. They don't talk to each other, they don't understand each other. Because we will fight on a joint and combined battlefield, we must work to resolve this deficiency.

One of the critical enablers in using information technology to enhance lethality, survivability, and the ability to manage the tempo of the battlefield is *adaptive command and control*. What elements of materiel can we interject to facilitate command and control on a digital battlefield?

First, we must be hesitant to impose too much standardization on commanders. How he does arrange his TOC? How does he work information flow in his organization? It is critical to give him the information in a format and a presentation that he can use and feel comfortable with—or else he won't use it.

Remember, we are dealing with human beings as we work the application of the technology. If we don't take into consideration the human dimension, in this case the personal needs of the commander, we won't realize the full utility of the new materiel.

> Nothing has, nor will, preclude the need for the commander to go forward, to fight from the front.

We must also acknowledge that even though Moore's Law is in effect, and that the speed of processors will double every 18 months, the human being on tomorrow's battlefield will look a lot like the human being on yesterday's and today's battlefields. His processing capacity didn't double. The human-computer interface must be considered.

Nothing has, nor will, preclude the need for the commander to go forward, to fight from the front. He must be in a position to see first hand what's happening at the critical point in the battlefield. His subordinates want to see him forward, being part of the action at hand. He must smell the cordite, share the hardships—all the things that extremely effective commanders have done over the past centuries. While in the pursuit of information technology, we must emphasize how to get the information to the commanders, and not force the commanders to be wedded to their TOCs.

We must concentrate on developing mobile command and control platforms. Commanders must constantly have access to critical information, and they must be able to move freely around the battlefield. *Mobile command and control is the critical enabler.* There is a requirement for the digital unit commander to be able to command and control from both ground and air platforms. Currently, two ongoing programs address this requirement: Command and Control Vehicle (CCV) and Army Airborne Command and Control System (AACCS).

We must continue to work to get the commander what he needs wherever he

is, and not require him to return to his TOC to get that information. The essence of what the commander needs is simple:

> We must develop tools to help the commander visualize the battle.

- First and most important, he must have the status of the answers to the information requirements he articulated, both enemy and friendly.

- Then he must be able to see on a single screen an integrated Red and Blue picture. Where are the enemy and friendly units in his battlespace?

- In addition, he must have visibility on all those things that influence his scheme of maneuver in his area of operation. Where are the natural obstacles, chokepoints, enemy minefields, enemy chemical strikes, etc.? This must be one screen, tailorable to the size of the battlespace so the commander can choose to focus on any point in time.

We must avoid the tendency to "filter information" before it gets to the commander. If the piece of information addresses specifically what the commander has asked for in his information requirements, then we must get it to him in the format he desires. We must get expert agents to help us manage information. We must develop systems within our software that help package bits of information into useable groups. In addition, we must pursue agents that, given a historical database of what the enemy has done in the past, will help us "think like the enemy." Expert agents can capture pieces of information that aren't of use right now but will probably be important very soon (when the enemy does something you didn't expect him to do).

We must focus on collaborative planning tools. Collaborative planning tools allow commanders (or staff officers) at all levels to simultaneously share thoughts and ideas about ongoing or anticipated missions. The Division Commander, for example, can use a "John Madden Whiteboard" capability to sketch out his commander's intent and scheme of maneuver for all the brigade commanders to hear simultaneously while staying at their distant location. The subordinate commanders can then review for the group the current situation in their areas of the battlefield, and highlight issues from their perspective with the upcoming operation. This is, undoubtedly, powerful stuff.

In addition, we must develop tools to help the commander visualize the battle. This could come in the form of mission planning and rehearsal tools, as well as tools that allow the commander to share his vision with his subordinate commanders. Currently, we still are fixated on sand table rehearsals. Groups are gathered around large terrain boards, and we walk them through the battle as it progresses. Modern technology can provide us visualization tools. We must develop systems that help us visualize the battle, and then share the visualization with our subordinates. We must be able to carefully show them what's in our "mind's eye."

We must design our systems so that our soldiers can use, maintain, and fix them. I found that routinely our 74B (automation specialists) and 31U (communication specialists) could fix the high-tech systems, given the parts. We must avoid designing our systems so that everywhere we go, we deploy with "contractor battalions."

We must retain an analog capability in our TOCs for two primary reasons. First, we must remember Murphy's Law as it applies to technology: It isn't IF the technology will fail but WHEN will it fail. When it does fail, there must be an analog backup capability. In addition, for the foreseeable future, units will consist of a combination of subordinate units, some with a digital capability and some without. There is still a requirement for both FM radios and ABCS boxes. There is still a requirement for both digital screens and map boards. And, as a result of the preceding requirement, there is still a need to provide a sufficient number of soldiers to conduct both analog and digital operations in command and control centers.

We must have a built-in redundancy in our command and control nodes. We must give the enemy credit: he is smart enough to look at us and determine what our capabilities and vulnerabilities are. He knows that he must disrupt our ability to command and control digitally; and as a result, he is going to focus his assets to disrupt our command and control. He is going to consider our command posts to be high payoff targets—our command posts will be extremely vulnerable. I would propose designing two identical TOCs for 1BCT operations—a "hot" command post and a "cold" command post, if you will. Each command post would have the same capabilities. The command post where the commander is closest to would be designated the hot command post. The cold command post would shift to the place on the battlefield where the commander would most likely need to be next.

> We must have a built-in redundancy in our command and control nodes.

And we mustn't forget the importance of eavesdropping. The advantage of FM communications is our ability to "eavesdrop" on other folk's nets to understand what's going on in their part of the battle. Current ABCSs don't allow you to do that. This is all part of the critical aspect of information technology: information sharing. Some people believe that the end-state is a "quiet TOC," an environment where everyone is wearing headsets and staring at computer screens. The problem is that no one shares information when they are wedded to their particular box.

Very soon we must work through all programs (Department of Defense, academia, and industry) and sort out the ones that aren't bearing fruit. I use the flower garden analogy. When a gardener wants to grow flowers, he ensures that he has enough fertilizer to make them all grow. If he has too many flowers, and not enough fertilizer, all the flowers will wither and die. None of them will get enough fertilizer to flourish. What the gardener must do is pull those flowers that aren't flourishing. This allows the limited amount of fertilizer he does have to concentrate on the other flowers.

Myths of Digital Technology

As we work our way into the future and focus on the potential military application of information technology, we must not allow ourselves to get overly enamored with the potential military application of information technology. There are several concepts in vogue these days that I will refer to as "Myths of Information Technology." Allow me work to work my way through four of these dangerous myths.

Myth #1 — TOCs will get smaller using information technology

This will be true—eventually. Now, however, we find that TOCs are getting bigger rather than smaller. They take more soldiers to man them, they have a larger footprint (both physically and electronically). Existing technology isn't totally reliable. Remember—it isn't IF the technology will fail you but WHEN. Commanders must equip, man, and train their TOCs to be able to command and control both digitally and in an analog fashion.

Staffs must track the battle. To do this in an analog environment, we had soldiers acting as radio-telephone operators (RTOs). They took the radio spot report from the subordinate units, and then passed the information to a soldier who posted that information. If the spot report was about a change in enemy or friendly locations, the soldier turned to the map and moved the "stickie" to replicate the most recently reported position.

In a digital TOC, those reports come over the ABCS. Subordinate units send changes to friendly positions over the MCS and changes to enemy positions over the ASAS. This information automatically updates all "addresses" with the new information. The people in the TOC simply see the new information when they look at their screens.

But what happens if, during the heat of the battle, the screens suddenly go blank. If a power surge destroys the systems? If the enemy was able to interdict the tactical internet? Or if a soldier touched the wrong button, or pulled the wrong wire, and the ABCSs stopped working? If the TOC doesn't have an analog backup to the digital systems, it would be clueless as to what was happening on the battlefield—and of no use to the commander.

In addition, units are composed of both digital and analog subordinate units. In the 1BCT during our NTC rotation, we had attached a light infantry battalion from Hawaii, and a Chinook element from the California National Guard. This isn't unrealistic. We won't get to the point of the battlefield anytime soon where everyone is digital. TOCs have to be able to process some information digitally and some analog.

In short, the requirement to be able to command and control both digitally and analog causes TOCs to get bigger, not smaller, at least in the near term. We need the digital systems and their assigned operators as well as the analog systems and their assigned operators. It is important to note that both of these functions require dedicated soldiers. For example, a soldier can't be both the RTO and an MCS operator—it just doesn't work.

Myth #2 — Training will take less time

Some people believe that it is easier, using information technology, to train individuals and teams to do their missions. In fact, there are groups who advocate that the technology is the panacea for a poor training program. All wrong.

As cited in previous chapters, training on information technology systems requires a three-step process:

➤ First, we must train the individuals and teams on the basics of being soldiers—the blocking and tackling, if you will.

➤ Then we must train them on the technology. How does it work, what are its capabilities and limitations?

➤ Then we must train them on the application of the technology. How can we apply what we now know about the new technology to how we improve our lethality, survivability, and ability to manage the tempo of the battlefield?

Every piece of the training program takes our most valuable resource—time. Training on the basics, the blocking and tackling, still requires what it has always required. Focus on the individual tasks during sergeant's time training. Focus on the collective tasks during lane training, etc. Taking soldiers and units over to a consolidated training facility, or to their motor pools for that matter, to learn a new piece of "kit." (We have always referred to this as New Equipment Training—and it takes time.) Then the application of the technology to basic warfighting takes time.

In the near term, it will take longer to train a unit that has information technology available than it does to train a similar analog unit. And nothing will ever take the place of a good, solid training program that is focused on the fundamentals, grounded in the basics—common sense training.

Myth #3 — We need "contractor battalions" to support us

Early in the evolution of information technology, everywhere we went we had to have contractors available to support us. They were the ones who had the parts and the knowledge to troubleshoot and repair the digital systems.

We are growing past this. We found in the 1BCT that our soldiers (our 74Bs, the computer automation specialists, and our 31 series, the communications specialists) could troubleshoot problems and diagnose faults with the best of the contractors. As stated earlier, these soldiers immersed themselves in the technology, and figured out how to best use and repair it.

The problem was the soldiers didn't have access to repair parts. On many occasions, our soldiers told the contractor what was wrong with their system and what part they needed. The contractor would get the part, and give it to the soldier who would then fix the system.

We must be very careful with the idea of relying on "contractor battalions" to support us in every contingency. Clearly they were critical in the early evolution of the technology. Now, however, we must concentrate on "growing our own" maintainers, soldiers who wear the uniform and who can always be counted on to be available when needed.

Myth #4 — Digitization will show us an immediate impact on battlefield operations

This is probably the most dangerous of all the myths. People are touting that information technology is going to show an immediate impact on our ability to conduct warfighting. They are trying to convince the world that information technology will show immediate improvements in lethality, survivability, and the ability to manage the tempo of the battle. But after hearing all these pronouncements, we conduct a major test and these so-called improvements aren't obvious.

In July 1999, the Government Accounting Office published a report titled *Battlefield Automation—Performance Uncertainties Are Likely When Army Fields Its First Digitized Division*, with references to the lack of obvious improvement in tactical operations:

> In our opinion, the efforts thus far designed to measure force effectiveness have produced inconclusive results, with maneuver units in the field showing no significant increase in lethality, survivability, and operational tempo while modeling and simulation do show increases.[1]

Why we aren't seeing obvious increases in force effectiveness in live experiments? Two primary reasons:

- ➤ Technology is still in its infancy. It isn't reliable, nor is it easily sustainable. Parts are hard to come by. Systems do crash without any apparent reason.

- ➤ Units still lack the time to train on the systems. Training has always been and always will be "Job One." We must take the time to train on the systems.

A perfect case in point was the FBCB2 limited user test in which the 1BCT participated in August 1998. A decision was made by the Division Commander to freeze hardware and software changes on January 1, 1998, which gave the team seven months to train using the three-step process. (We first trained on the basics (the blocking and tackling), then we trained on the technology, then we applied the technology to the basic warfighting.) By August, we were proficient, and the results of the limited user test showed the effectiveness of the FBCB2 system. During the last fight, a Mechanized Infantry Task Force, equipped with FBCB2, totally destroyed an Armor Task Force, only losing one Bradley Fighting Vehicle during the course of the fight.

We used the technology the way it was intended. Forces were dispersed over 15 kilometers, and combat power was concentrated at the time and place of their choosing. The Mechanized Infantry Task Force could do that because the leaders of that task force all had situational awareness and understanding, provided by FBCB2. This occurred because we had taken the time to train.

Finally, we must be very careful not to conduct live experiments with information technology when the tested unit has not had time to adequately train. Technology isn't the panacea for a poor training program.

---

[1] Government Accounting Office, July 1999, GAO/NSIAD-99-150, p. 14.

Conclusions

We are on an extremely interesting and important journey—the journey to take advantage of the power of information technology in order to improve the lethality, survivability, and ability to manage the tempo of the battlefield of our Army. We have been working our way through the issues associated with this important endeavor for many years now. Every day, we get closer to the desired end-state. We learn. We adjust. We go forward.

We must proceed from this point forward, capitalizing on lessons that have already been learned. As people come and go in digital organizations, let's take the time to first review what we have already learned, and build on that. Let's stop "starting with a clean sheet of paper."

We must focus on the T-L-S elements of the imperatives—training, leader development, and soldiers, the essence of which will enable us to access the power of the technology sooner rather than later. Too many times we rush to the Materiel imperative and convince ourselves that we can improve operations simply by providing operational units with new hardware and software. Wrong answer!

> We must focus on the T-L-S elements of the imperatives—training, leader development, and soldiers.

We must take time to develop the individual (especially the leader) and ensure that he has the necessary SKAs to truly leverage the technology. We must take the time to allow units to train—individually and collectively—on first the basics, and then on the application of the technology to improve their warfighting prowess.

And we must focus on mobile command and control. We must get the information to the commander wherever he is on the battlefield. We must not force the commander to come back to the rear to get the information. Warfighting is still about people. The commander must be forward, smelling the cordite, hearing the sounds of the battlefield, and talking face to face with his soldiers. We must work hard now to get the commander the ability to command and control, using digital systems, from anywhere on the battlefield.

Acronyms and Abbreviations

AACCS	Army Airborne Command and Control System
AAR	after-action review
ABCS	Army Battle Command System
AFATDS	Advanced Field Artillery Tactical Data System
ASAS	All Source Analysis System
1BCT	1st Brigade Combat Team (4th Infantry Division, Ft. Hood, Texas)
BRT	Brigade Recon Troop
CCV	Command and Control Vehicle
CSM	Command Sergeant Major
CSS	Combat Service Support
DOTLMS	doctrine, organization, training, leader development, materiel, and soldiers
DTG	Date-Time Group
EEFI	Essential Elements of Friendly Information
EPLRS	Enhanced Position Location Reporting System
FBCB2	Force XXI Battle Command Battalion/Brigade and Below
FSO	Fire Support Officer
FSB	Forward Support Battalion
FSC	Forward Support Company
GED	General Equivalency Diploma
GT	General Test
HVA	high-value asset
IDA	Institute for Defense Analyses
JAWP	Joint Advanced Warfighting Program
JSTARS	Joint Surveillance Target Attack Radar System
LNO	liaison officer
MCS	Maneuver Control System
MLRS	Multiple-Launch Rocket System
MOS	military occupational specialty
MSE	Mobile Subscriber Equipment
NAI	named areas of interest
NCO	non-commissioned officer

NTDR	Near Term Digital Radios
NTC	National Training Center
OC	observer/controller
OER	officer efficiency report
OPFOR	opposing force
PIR	Priority Information Requirements
PT	physical training
RTO	radio-telephone operators
SINCGARS	Single Channel Ground and Airborne Radio System
SKAs	skills, knowledge, and attributes
SOP	standing operating procedures
TACSOP	tactical standing operating procedures
TAI	Targeted Area of Interest
TOC	Tactical Operations Center
TTP	tactics, techniques, and procedures
UAV	unmanned aerial vehicle
US	United States
USA	United States Army

Notes

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE June 2001	3. REPORT TYPE AND DATES COVERED Final

4. TITLE AND SUBTITLE Lessons Learned: Commanding a Digital Brigade Combat Team	5. FUNDING NOS. DASW01-98-C-0067 AI-8-1627

6. AUTHOR(S) Rick Lynch	

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Joint Advanced Warfighting Program Institute for Defense Analyses 1801 N. Beauregard Street Alexandria, VA 22311-1772	8. PERFORMING ORGANIZATION REPORT NO. IDA Paper P-3616

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Deputy Under Secretary of Defense for Advanced Systems and Concepts Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics 3700 Defense Pentagon Washington, DC 20301-3700	10. SPONSORING/MONITORING AGENCY REPORT NO.

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, unlimited distribution: July 17, 2001.	12b. DISTRIBUTION CODE 2A

13. ABSTRACT (Maximum 200 words)

This paper describes the experiences of the author as commander of the 1st Brigade Combat Team, 4th Infantry Division, at Fort Hood, Texas. The 1BCT was engaged in a series of training events and experiments that focused on the potential application of information technology to military operations. Organized along the lines of DOTLMS (doctrine, organization, training, leader development, materiel, and soldiers), the paper highlights issues that a digital organization faces in addition to basic issues still unresolved in the US Army. Among the lessons learned: technology isn't a panacea for poor training; transform every experiment as much as possible into a training event; retain soldiers with critical, highly technical skills; place leaders in stressful, demanding situations, and evaluate their responses; train soldiers in the basics first before turning their attention to new technology; plan the communications backbone first; use collaborative planning tools when conducting simultaneous, complex operations; and always have an analog backup to digital operations. The author discusses four of the dangerous myths of digital technology, and concludes with recommendations.

14. SUBJECT TERMS Collaborative planning tools, command and control, communications, counseling, digitalization, doctrine, training, experimentation, information technology, interoperability, leader development, materiel, military operations, organization, soldiers.	15. NO. OF PAGES 50
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL